BLUEBEAM TECHNICAL SUPPORT

Single Sign-on Integration Request

Complete this request for single sign-on (SSO) configuration. Upon submission, a Bluebeam representative will review your request. You'll be notified if any further information is required.

To be eligible for SSO integrations, your organization must have an active Bluebeam subscription plan for your organization. Other limitations may apply. Please contact a sales support representative for more details.

Account Information

Company:

Subscription SN:

Primary SSO Integrations Admin Name:

Primary SSO Integrations Admin Email:

Studio Prime

If your organization is utilizing Studio Prime integrations, we won't be able to proceed with SSO enablement. The authentication that Studio Prime integrations use is not compatible with SSO.

Please confirm if your organization uses Studio Prime with Integrations.

- ☐ Studio Prime is currently being used with integrations.
- ☐ Studio Prime is currently being used without integrations.
- ☐ Studio Prime is not being used in our organization.

Authentication

Currently, Microsoft Azure Active Directory (Azure AD) and the Okta AD federated identity infrastructure, using the OpenID Connect (OIDC) protocol, are the two supported SSO platforms.

Please select the Authentication platform that will be used for SSO integration.

- ☐ Microsoft Azure AD
- ☐ Okta Identity Infrastructure

Please select the server region(s) for which SSO integration will be implemented.

(Check all that apply)

- ☐ AU - Australia
- ☐ DE - Germany
- ☐ SE - Sweden
- ☐ UK - United Kingdom
- ☐ US - United States

Submit the Form

1. Please email this completed request to support@bluebeam.com.
2. Upon completion of this form, you'll be given access to fill out your SSO Admin profile in our accounts page. This is where you can configure further information about your organization related to SSO and submit a list of domains to configure. An active Bluebeam ID (BBID) is required, please create one following the suggestions here if you haven't already done so.

   IMPORTANT: You must log into our accounts page and fill out the SSO Admin profile, including the list of your domains, before we can provide you with an audit list of Studio users in your organization. We provide this to ensure that the users in the identity server match users tied to subscriptions and Bluebeam products.

Please double check for any errors in your requested domains list. We cannot be responsible for any typos or mistakes that could lead to domain access issues for your users.

Frequently Asked Questions

I've submitted my request form, what are the next steps?

The next set of steps can be broken down into things Bluebeam will do and things that you must do. Please note that this process is hardly ever quick and may take some time to complete.

1. We'll configure your SSO Admin account that you provided above, with access to a new profile area that you must fill out. It expresses key SSO identifier information such as client IDs and domains needed to configure your account. Once you fill it out, we're automatically notified and will start generating a list of current users associated with your domains.
2. Before SSO is enabled, you'll need to audit the list of Studio users in our system with those listed in your identity provider. Please audit the list carefully.

   IMPORTANT: Your users' BBIDs must match their entries in Microsoft Azure Active Directory (AD) or their usernames in Okta (depending on which identity provider your organization uses) to ensure they retain access to all the Sessions, Projects, and other Studio work they spent valuable time creating. If they attempt to access our services but do not match their values registered with your identity provider, they will no longer be able to see their existing Sessions and Projects, and you must contact Technical Support to coordinate efforts to resolve those out-of-sync user accounts.
3. Once you've worked on your end to reconcile your users in preparation to migrate to SSO, you'll communicate back to us that you're ready to proceed with either testing, or full domain transition to SSO. We recommend testing on either a sub domain or on a subset of users.
4. If testing is successful, we'll schedule with you an appropriate time to perform the migration. Once a migration is completed, all users attempting to access our services with an email address associated with your domains will be swapped over to SSO.

Do you support other platforms aside from Azure or Okta?

Currently, we only support the following:

- Microsoft Azure
- Okta Identity Infrastructure

How should our accounts be configured for SSO?

It is required that SSO be configured/mapped to an email address for the Account Sync process to work correctly. If an alternative configuration/mapping is requested or required, it must represent an **Email** value defined in your Active Directory.

Any value other than the **Primary Email Address** will not be compatible with the SSO configuration.

I have Studio Enterprise; can I still use SSO?

Yes, separate login screens will be used to access the license subscription in Revu and the Studio Enterprise server.

Users will continue using their existing credentials to access Studio Enterprise. It's not possible to integrate SSO with Studio Enterprise.

Is SSO region specific?

Yes, SSO will be set up for each region individually. This is to secure sensitive information pertaining to accounts in certain regions.

Why should I reconcile my user list before implementing SSO?

There may be existing users who'll no longer have access to Bluebeam services unless their information is corrected. A list of all users tied to your specified domain(s) will be provided for you to reference. We provide this to ensure that the users in your database match the records tied to your subscriptions and Bluebeam services.

Potential discrepancies between the Bluebeam ID list we provide and your Active Directory userbase:

- The Bluebeam ID (email) doesn't exist in the Active Directory
- Terminated employees, alias/nickname emails used as an alternative to the Active Directory email
- The email changed in the Active Directory and is no longer the same as the Bluebeam ID
- Typos with the Bluebeam ID that differ from what's registered in the Active Directory
- And other unexpected authentication problems that may prevent a successful implementation

There are discrepancies within my audit list and Active Directory. What should I do?

You're responsible for your organization's accessibility after SSO is enabled. Our recommendation would be to ensure that any user within the audit list matches their credentials for Active Directory. For users that need to make changes and reconcile their accounts, please have them make changes at https://accounts.bluebeam.com/.

How are SSO changeovers coordinated and scheduled?

Our priority is to maintain the integrity of our services to all our customers, followed closely by identifying a window that has a minimal transitional impact to your users. We factor in the number of active users across our systems, along with the overall volume of activity from your organization to determine an appropriate changeover window with you.

What can our users expect to happen during and/or immediately after the changeover?

The transition process first removes their existing authentication credentials and replaces them with your users' SSO-based credentials. This change will be seamless for all users, except for those actively logged in with existing non-SSO credentials. Those users will not benefit from SSO until they sign out, and then sign in again with their SSO-based credentials.

To ensure all your users sign in with SSO-based credentials after the changeover, we recommend that you alert them to sign out of their Bluebeam services prior to the scheduled changeover, and then sign back in with their SSO-based credentials after the changeover is complete.

After we transition to SSO, what happens when we remove a user from our Active Directory?

When a user is removed from the Active Directory, any attempts for them to log in to our solutions or services using the email that was removed will fail. However, this doesn't deprovision the entitlement from our license system. To reclaim your entitlement, simply log into the Bluebeam Licensing Org Admin Portal, search for the user that was removed, and then deactivate them.

What identity federation/protocol does Bluebeam use?

OpenID Connect (OIDC) protocol.

What user provisioning is used for SSO?

Bluebeam uses Just-in-Time (JIT) provisioning with OpenID connect.

Do you support SCIM (System for Cross-domain Identity Management)?

SCIM is not currently supported, but it is on our roadmap and there are plans to support this soon.